Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is a process that helps an organisation identify and minimise the data protection risks of a project.

Version Control

Version	Reason	Date	Author(s)
0.1	Draft - initial draft	21/3/22	Sarah Laws
0.2	Amended	28/3/22	Sarah Laws
0.3	Reviewed and commented	29/3/22	[redacted] and [redacted]

Project / Work Stream Name	**Supporting Families DSA**
Overview: **(Summary of the project/work stream)**	This DPIA is for the Supporting Families DSA. This covers the sharing of limited information about data subjects where it has been identified that they are eligible to receive support for the supporting families scheme under the Department of Levelling Up, Housing and Communities (DLUHC) Supporting Families Framework and stipulated within the DLUHC approved outcomes plan.
Implementation Date:	Sharing ongoing, DSA from 1/4/22
Environmental Scan Describe the consultation/checks that have been carried out regarding this initiative or, project of similar nature, whether conducted within your organisation or by other organisations.	Supporting Families work is carried out nationally and there is a central government/councils DSA to cover sharing between them, which is not covered by this DSA. There may be local fragmented DSAs but no single pan-London coordinated DSA. It should be noted that only the data specified in this DSA is covered by this particular DSA. Other information will be shared between councils, the Police, and other partners which is used for wider purposes including safeguarding, family interventions, and similar work, and which may be undertaken by teams in councils undertaking troubled/supporting families type work. This will be covered in other DSAs This DSA covers the personal and criminal offence data to be shared. It is not anticipated that special category data (sensitive data under Part 3) will be shared

Step 1: Complete the Screening Questions			
Q 1	**Category**	**Screening question**	**Yes/ No**
1.1	Technology	Does the project introduce new or additional information technologies that can substantially reveal an individual's identity and has the potential to affect that person's privacy?	No
1.2	Technology	Does the project introduce new or additional information technologies that can substantially reveal business sensitive information, specifically: have a high impact on the business, whether within a single function or across the whole business?	No
1.3	Identity	Does the project involve new identifiers, re-use or existing identifiers e.g. NHS or NI number, Local Gov. Identifier, Hospital ID no. or, will use intrusive identification or identity management processes or, electronic linkage of personal data?	Yes
1.4	Identity	Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?	No
1.5	Multiple organisatio ns	Does the project involve multiple organisations, whether they are public sector agencies i.e. joined up government initiatives or private sector organisations e.g. outsourced service providers or business partners?	Yes
1.6	Data	Does the project involve new process or significantly change the way in which personal data/special categories of personal data and/or business sensitive data is handled?	No
1.7	Data	Does the project involve new or significantly changed handling of a considerable amount of personal data/special categories of personal data and/or business sensitive data about each individual in a database?	No
1.8	Data	Does the project involve new or significantly change handling of personal data/special categories of personal data about a large number of individuals?	No
1.9	Data	Does the project involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal data/special categories of personal data and/or business sensitive data from multiple sources?	Yes
1.10	Data	Will the personal data be processed out of the EEA?	No
1.11	Exemptions and Exceptions	Does the project relate to data processing which is in any way exempt from legislative privacy protections?	No
1.12	Exemptions and Exceptions	Does the project's justification include significant contributions to public security and measures?	No
1.13	Exemptions and Exceptions	Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?	No

The purpose of the screening questions is to confirm that the data protection laws are being complied with, or highlights problems that need to be addressed. It also aims to prevent problems arising at a later stage which might impede the progress or success of the project.**Answering "Yes" to any of the screening questions above represents a potential Information Governance (IG) risk factor, please proceed and complete the next section.**

Step 2: Identify the need for a DPIA										
2.1	**Is this a new or changed use of personal data/special categories of personal data and/or business sensitive data that is already processed/shared?**							New/Changed		
								Changed		
2.2	**What data will be processed/shared/viewed?**									
	Personal Data									
	Forename	**yes**	Surname	**yes**	Date of Birth	**yes**	Age	**yes**	Gender	
	Address	**yes**	Postal address	**yes**	Employment records		Email address	yes	Postcode	**yes**
	Other unique identifier (*please specify*)	**yes eg case management system ref number**	Telephone number	**yes**	Driving licence number		NHS No		Hospital ID no	
	Other data *(Please state):*									
	Special Categories of Personal Data NONE									
	Racial or ethnic origin		occasionally	Political opinion		Religious or philosophical beliefs				
	Trade Union membership			Physical or mental health or condition						
	Sexual life or sexual orientation		occasionally	Social service records		Child protection records				
	Sickness forms		Housing records		Tax, benefit or pension records		Adoption records			
	DNA profile		Fingerprints		Biometrics		Genetic data			
	Special category data is not routinely shared under this DSA. However occasionally data that identifies race or sexuality may be shared indirectly where a child eg identifies as LGBT+ and requires support. **Proceedings for any offence committed or alleged, or criminal offence record** ● Whether data subject is involved in or convicted of a crime ● The quarter that involvement/conviction took place ● Whether the data subject is a victim or subject									**yes**

	Other data *(Please state):*		
	Will the dataset include clinical data? (please include)		**Yes/No**
			no
	Will the dataset include financial data?		No
	Description of other data processed/shared/viewed?		

2.3	**<u>Business sensitive data</u>**			
	Financial	No		
	Local Contract conditions	No		
	Operational data	No		
	Notes associated with patentable inventions	No		
	procurement/ tendering information	No		
	Customer/ supplier information	No		
	Decisions impacting:	One or more business function		**Yes/No**
				No
		Across the organisation		No
	Description of other data processed/shared/viewed (if any).			
	N/A			

<table>
<tr><th colspan="4">Step 3: Describe the sharing/processing</th></tr>
<tr><td rowspan="5">3.1</td><td colspan="2">List of organisations/partners involved in sharing or processing personal/special categories personal data? If yes, list below</td><td>Yes/No</td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td>Name</td><td>Controller or Processor?</td><td>Completed and compliant with the IG Toolkit or Data Security and Protection (DSP) Toolkit
Yes / No</td></tr>
<tr><td>London Local Authorities</td><td>Controller</td><td>Yes</td></tr>
<tr><td>Metropolitan Police Service and City of London Police</td><td>Controller</td><td>Met: Yes, CoLPS No but other equivalent assurances in place</td></tr>
<tr><td rowspan="2">3.2</td><td rowspan="2">If you have answered ‘yes’ to 3.1 is there an existing ‘ Data Processing Contract’ or ‘Data Sharing Agreement’ between the Controller and the Processor?</td><td colspan="2">Yes/No</td></tr>
<tr><td colspan="2">Yes - This DPIA is for the DSA to cover this sharing.</td></tr>
<tr><td>3.3.</td><td>Has a data flow mapping exercise been undertaken?
If yes, please provide a copy, if no, please undertake</td><td colspan="2">The flows will vary case by case according to specific circumstances and case requirements</td></tr>
<tr><td rowspan="2">3.4</td><td colspan="2" rowspan="2">Does the project involve employing contractors external to the Organisation who would have access to personal or special categories of personal data?</td><td>Yes / No</td></tr>
<tr><td>No</td></tr>
<tr><td rowspan="2">3.5</td><td colspan="3">Describe in as much detail why this information is being processed/shared/viewed?
(For example Direct Patient Care, Statistical, Financial, Public Health Analysis, Evaluation. See NHS Confidentiality Code of Practice Annex C for examples of use)</td></tr>
<tr><td colspan="3">To deliver the best decisions that ensure timely, necessary and proportionate interventions, decision makers need the full picture concerning an individual and their circumstances. This data sharing agreement aims to support and improve the welfare of families by identifying those with multiple complex problems and addressing their needs through systemic joined up working and intervention.

See intro above which explains the limited scope of this DSA and that other information relevant to practitioners in this area is likely to be shared between agencies under different DSAs. This DSA covers only the personal data described above. However, practitioners will find they receive and share additional personal data from and with other agencies relating to families under other DSAs.</td></tr>
</table>

	Information viewed alone or in silos may not give the full picture or identify the true risk. All the information from various agencies needs to be available and accessible in one place; to keep local residents and other stakeholders safe and assist signatories to this Agreement in discharging their obligations under the Act and other legislation. Data sharing will enable the parties to use analytical techniques to identify families who are most at risk, vulnerable or likely to have negative outcomes. This means informed decisions can be made to target limited resources, which will allow the parties to facilitate enhanced assistance to the mutual benefit of families and public services as part of a prevention strategy. Proactively introducing this support to families encourages more positive outcomes and prevents the use of crisis services and long-term poor outcomes. This allows families to be more self-sustaining and less reliant on the state. The support provided aims to achieve “significant and sustained progress”' with the families and prevent households from being drawn into different types of crime like anti-social behaviour, domestic violence and abuse. Progress is determined locally with key stakeholders in line with DLUHC Guidance.

Step 4: Assess necessity and proportionality	
4.1	**Lawfulness for Processing/sharing personal data/special categories of personal data?** **For Local Authorities** **Article 6 (1) – Personal Data Processing:** (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller Data Protection Act section 8 requirements are met by : Digital Economy Act 2017 part 5 and associated codes of practice - this is the main law The Children Act 1989 The Children Act 2004 The Children & Social Work Act 2017 The Crime and Disorder Act 1998 The Care Act 2014 **Article 9 (2) – Special Category Personal Data Processing It is not anticipated that special category data will be shared under this DSA**. However if it is, as discussed in 2.2 above, then the legal basis will be Article 9(g) substantial public interest - processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject Use of this article requires that the Data Protection Act Section 10(3) be satisfied. This requires that a condition within Schedule 1, Part 2 is met. For this agreement these are: ● Statutory etc., and government purposes under Para 6(1)(2) ● Preventing and detecting unlawful acts under Para 10(1)(2)(3) ● Safeguarding children and individuals at risk under Para 18(1)(2)(3)(4) **Art. 10 UK GDPR : Processing of personal data relating to criminal convictions and offences** Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. The art 6 legal basis is above. The Data Protection Act 2018 Schedule 1 condition: ● Part 1 para 2(1) Health or social care purposes: This condition is met if the processing is necessary for health or social care purposes… (e)the provision of social care Part 2 para 6 Statutory etc and government purposes: 6(1) This condition is met if the processing— (a)is necessary for a purpose listed in sub-paragraph (2), and (b)is necessary for reasons of substantial public interest. (2) Those purposes are— (a)the exercise of a function conferred on a person by an enactment or rule of law; Preventing or detecting unlawful acts

2.4.2 For the purposes of law enforcement by competent authorities (Metropolitan Police)

The “competent authorities” are defined in Section 30 of the DPA which refers to Schedule 7. The competent authorities under this agreement are generally (but not exclusively) police, youth offending teams and government departments.

The “law enforcement” purposes are defined in Section 31 of the DPA as “prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security”.

There are additional safeguards required for “sensitive processing”. This is defined in Section 35(8) as:

a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
c) the processing of data concerning health;
d) the processing of data concerning an individual’s sex life or sexual orientation.

it is not anticipated that such information will be shared under this DSA. However, if it should be then the additional requirements are given in Section 35(4) and (5). Both require an appropriate policy document, and this document will form part of the policy for such processing, although competent authorities will need to satisfy themselves that their own internal policy documents fully cover such use.

Section 35(4) requires the consent of the data subject, which is not applicable.

35(5) requires that the processing be strictly necessary for law enforcement purposes, and meets a condition in Schedule 8.

For the processing in relation to the purposes here, the following conditions in Schedule 8 are met:

- Statutory etc. purposes Para 1(a)(b);
- Administration of justice Para 2;
- Protecting individual’s vital interests Para 3;
- Safeguarding of children and of individuals at risk Para 4(1)(2)(3)(4);

4.2	**Will the information be processed/shared electronically, on paper or both?**	Electronic	Yes
		Paper	Possibly

4.3 How will you ensure data quality and data minimisation?

Each partner is responsible for ensuring the accuracy and relevance of the personal data that it processes and shares and must have clear processes in place for managing data quality.

Any party learning of the inaccuracy of personal data is responsible for taking appropriate action to correct it and informing the parties with whom that data has been shared.

4.4	**Have individuals been informed about the proposed use of their personal or special categories of personal data?** *For example, do the organisations/partners listed in section 3.1 have updated Fair Processing Notice available to patients on their websites?*	Yes

	Privacy notices for all organisation note these purposes. However, in some cases, data subjects may not be specifically notified about the use of their data where giving them this information would be impossible or involve disproportionate effort.	
4.5	**How will you help to support the rights of individuals?**	
	Each controller remains responsible for complying with the applicable data subject rights. Each controller has their own documented policies and procedures which details how they will meet their own obligations in respect of data subject rights.	
4.6	**Are arrangements in place for recognising and responding to Subject Access Requests (SARs)?**	
	Each controller remains responsible for their own data subject requests. Where a SAR covers data provided by another party, before responding to the SAR, the Controller will consult with the providing party regarding any disclosure concerns they may have.	
4.7	**Will the processing of data include automated individual decision-making, including profiling?** *If yes, please outline the profiling processes, the legal basis underpinning the process, and the rights of the data subject*	No
	N/A	
4.8	**Will individuals be asked for consent for their information to be processed/shared?** *If no, list the reason for not gaining consent e.g. relying on other lawful basis, consent is implied where it is informed.*	No
	The parties will often work collaboratively with data subjects and aim for agreement with them on the actions to be taken. However, it is recognised that this is different to using consent (Article 6 (a)) (or explicit consent (Article 9 (a))) as the lawful basis conditions used for processing under this agreement. Consent is not generally the lawful basis the public sector organisations use for processing information shared under this agreement. It is noted that where consent is not the lawful basis for processing, consent does not need to be sought to share, and thus the concept of "overriding consent" is a misconception. Lawful basis is set out in detail above	
4.9	**As part of this work is the use of Cloud technology being considered either by your own organisation or a 3rd party supplier? If so please complete the embedded questionnaire.**	Existing technologies are used, no new systems.
4.10	**Where will the data be stored** *Examples of Storage include bespoke system (e.g. EPR, Emis & other clinical systems, SharePoint, data repository, Network Drives, Filing cabinet (office and location), storage area/filing room (and location) etc.*	
	Provider systems are used. Paper storage is minimised; all storage is UK only.	
4.11	**Data Retention Period** *How long will the data be kept?*	
	Organisations are required by data protection legislation to document processing activities for personal data, such as what personal data is held, where it came from and with whom it has been shared. This Record of Processing Activity (ROPA) must include the retention period for the data.	

	Information must not be retained for longer than necessary for the purpose for which it was obtained. Disposal or deletion of personal data once it is no longer required, must be done securely with appropriate safeguards, in accordance with that organisation's disposal policies.	
4.12	**Will this information be shared/processed outside the organisations listed above in question 3?** *If yes, describe who and why:*	Yes/No
	If there is further sharing it will be under the existing arrangements for processing and sharing of data by the parties and not as a result of this DSA	Possibly

Step 5: Information Security Process

5.1	**Is there an ability to audit access to the information?**	Yes/No
	All DSPT certified provider systems have an audit built in.	Yes

5.2	**How will access to information be controlled?**					
	This varies but RBAC control is required with password access as minimum.					
5.3	**What roles will have access to the information?** (list individuals or staff groups)					
	Relevant professionals within the council/police teams					
5.4	**What security and audit measures have been implemented to secure access to and limit use of personal data/special categories of personal data and/or business sensitive data?**					
	Username and password	yes	Smartcard		key to locked filing cabinet/room	yes
	Secure 1x Token Access		Restricted access to Network Files			yes
	Other: *Provide a Description Below*:					

5.5	**Is there a documented System Level Security Policy (SLSP) or organisational equivalent for this project?**	Yes/No Not required, no new system.
5.6	**Are there Business Continuity Plans (BCP) and Disaster Recovery Protocol for the proposed/existing system or process?** *Please explain and give reference to such plan and protocol*	Yes/No YES

5.7	**Is Mandatory Staff Training in place for the following?**	Yes/No	
	● Data Collection:	YES	
	● Use of the System or Service:	YES	
	● Information Governance:	YES	
5.8	**Are there any new or additional reporting requirements for this project?**	No	

	● What roles will be able to run reports?	
	N/A	
	● What roles will receive the report or where will it be published?	
	N/A	
	● Will the reports be in person-identifiable, pseudonymised or anonymised format?	
	N/A	
	● Will the reports be in business sensitive or redacted format (removing anything which is sensitive) format?	
	N/A	
5.9	**Have any Information Governance risks been identified relating to this project?** (if Yes the final section will need to be completed)	**Yes/No** Yes

Step 6: Identify and Assess Risks			
Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Note: risks here are risks of this sharing ONLY. Signatories should have DPIAs for their own individual systems and methods, covering their local risks.			
Misuse of data: Personal data could be used by a recipient in a manner incompatible with the Data Sharing Agreement. This might be unauthorised uses or disclosure to inappropriate persons. The Supporting Families information does not contain any special category data, however it will identify children by name, address and age, and also show whether they have been involved in or convicted of a crime, and whether they are a victim. Young people are afforded special protections under the law. By virtue of being a victim or perpetrator the child is vulnerable. Harms could include embarrassment and distress, or being targeted for further attacks, reprisals and revenge. Compliance risk: Appropriate technical and organisational measures shall be taken. Corporate risk: Reputational risk. Loss of trust. Legal implications.	Medium	Very High	Very High
Loss of data in transfer. Personal data could be obtained and misused by third parties.Harms could include embarrassment and distress, or being targeted for further attacks, reprisals and revenge. Compliance risk: Appropriate technical and organisational measures shall be taken. Corporate risk: Reputational risk. Loss of trust. Legal implications.	Medium	High	Medium/high
Further transfer of data: Risk to the safety of personal data if transferred elsewhere by a recipient. The supporting family information is of a confidential nature (although not special category data) as explained in 'misuse of data' above. Harms could include embarrassment and distress, or being targeted for further attacks, reprisals and revenge. Compliance risk: Personal data shall be obtained for one or more specified and lawful purposes. Appropriate technical and organisational measures shall be taken. Personal data shall not be transferred outside the European Economic Area. Corporate risk: Reputational risk. Loss of trust	Medium	High	Medium/high
Disposal of data: If personal data is not disposed of in an appropriate manner by the party with whom it was shared, it may be possible for third parties to obtain the data causing	Medium	High	Medium/high

harm to the data subjects. Harms could include embarrassment and distress, or being targeted for further attacks, reprisals and revenge. Compliance risk: Personal data shall not be kept for longer than necessary.Appropriate technical and organisational measures shall be taken.Corporate risk: Reputational risk. Loss of trust. Legal implications.			
Inherent privacy intrusion: sharing of personal data is inherently privacy intrusive, especially for vulnerable people. As explained above the people in question are vulnerable and may be children. Compliance risk: data minimization, privacy intrusion Appropriate technical and organisational measures shall be taken.Corporate risk; Reputational risk. Loss of trust. Legal implications	High	High	High

Step 7: Identify Measures to reduce risk				
Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 6				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
Misuse of data:	Sharing will be by and to authorised officers only who are subjected to full employment checks. Access to all Partner systems are fully RBAC and auditable. All organisations have full employee policies and codes of conduct. Beaches of those would be a disciplinary offence and may be a criminal act.	Reduced	Low	Yes
Loss of data in transfer.	The DSA specifies the appropriate technical measures in place to ensure the security of the data transfers. Organisations have full policies and procedures in place for the safe transfer of data. The Partners routinely share volumes of special category data and have well established protocols to do so safely.	Reduced	Low	Yes
Further transfer of data:	It is noted that where one party receives data from another, the receiving party becomes a Data Controller and is then liable for their use of the data, and is bound by the requirements of data protection legislation. All parties have full policies	Reduced	Low	Yes

	and processes in place to ensure data is handled securely. Systems are auditable and RBAC is in force. Employees are subject to robust employment checks. However it is noted that where a Data Controller handles data in a manner not expected this can lead to reputational damage for the supplying party, notwithstanding they have no legal liability data protection wise. For this DSA it is considered these risks are low.			
Disposal of data	It is noted that where one party receives data from another, the receiving party becomes a Data Controller and therefore takes the liability for the data from that point, and is bound by the requirements of data protection legislation. All parties have their own data retention policies which they will follow.	Reduced	Low	Yes
Inherent privacy intrusion	The risk is the sharing with and by Partners **not** the existing processing for Supporting Families which are covered by other DPIAs. Privacy intrusion is unavoidable, otherwise the sharing could not be facilitated. The DSA requires that sharing will only be of data necessary in each instance and will be the minimum needed to achieve the lawful purposes. There is unlikely to be any special category data shared. The personal data, whilst of vulnerable people, is low level. Name/address may be publicly available and only through association with this programme takes on more significance. The criminal offence data will only apply to those who are victims or perpetrators so not all those whose data is processed.	Reduced	Medium	Yes

Residual Risk Level	**Medium**

Step 8: Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by:	[redacted], Information Governance Manager RBKC and Westminster CC, and [redacted], Data Protection Manager, LB Camden March 2022	Each Data Controller's Information Asset Owner to ensure they are satisfied by these
Residual risks approved by:	[redacted], Information Governance Manager RBKC and Westminster CC, and [redacted], Data Protection Manager, LB Camden March 2022	Each Data Controller's Information Asset Owner to ensure they are satisfied by these
DPO advice provided:	[redacted] Information Governance Manager RBKC and Westminster CC, and [redacted] Data Protection Manager, LB Camden March 2022	Each Data Controller's DPO to agree or provide own advice
Summary of DPO advice: *Please see the FAQs on how councils should adopt/adapt this DPIA or undertake their own.* This is assessed as medium risk. The remaining risk that is medium rather than low is the privacy intrusion. This is considered proportionate to the aims of the processing and bearing in mind the procedures and processes in place to ensure data minimisation, proportionality, and information security.		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		

This DPIA will kept under review by:	The DPIA will be reviewed by the respective DPOs of each organisation when required	The DPO should also review ongoing compliance with DPIA